What is claimed is:

1. A key scheduler for an apparatus using DES encryption algorithm, comprising:

a first permutation choice unit for permuting a 56-bit block;

a first register for storing left 28 bits among the 56-bit block from the first permutation choice unit in accordance with a clock signal;

a second register for storing right 28 bits among the 56-bit block from the first permutation choice unit in accordance with the clock signal;

a first and a second shift units for shifting the 28-bit blocks stored in the first and the second registers to the left by a first predetermined number of bits and outputting shifted 28-bit blocks to the first and the second registers respectively;

a second permutation choice unit for permuting the 28 bits stored in the first and the second registers, thereby generating a first subkey;

a third and a fourth shift units, each for shifting the 28 bits stored in the first and the second registers to left by a second predetermined number of bits; and

a third permutation choice unit for permuting the 28 bits stored in the third and the fourth shifters, thereby generating a second subkey.

2. The key scheduler as recited in claim 1, wherein the second predetermined number is one or two.

3. The key scheduler as recited in claim 2, wherein the third permutation choice unit is implemented by wiring.

4. A key scheduler for an apparatus using DES encryption algorithm, comprising:

a first permutation choice unit for permuting a 56-bit block;

a first register for storing left 28 bits among the 56-bit block from the first permutation choice unit in accordance with a clock signal;

a second register for storing right 28 bits among the 56-bit block from the first permutation choice unit in accordance with the clock signal;

a first and a second shift units for shifting the 28-bit blocks stored in the first and the second registers to the left by a first predetermined number of bits and outputting shifted 28-bit blocks to the first and the second registers respectively;

a second permutation choice unit for permuting the 28 bits stored in the first and the second registers, thereby generating a first subkey;

a third and a fourth shift units, each for shifting the 28 bits stored in the first and the second registers to right by a second predetermined number of bits; and

a third permutation choice unit for permuting the 28 bits stored in the third and the fourth shifters, thereby generating a second subkey.

5. The key scheduler as recited in claim 4, wherein the second predetermined number is one or two.

6. The key scheduler as recited in claim 5, wherein the third permutation choice unit is implemented by wiring.